CLASS SPECIFICATION
County of Fairfax, Virginia

CLASS CODE: 1831 **TITLE:** INFORMATION SECURITY ANALYST II **GRADE:** S-27

DEFINITION:
Performs, with minimum supervision, information protection work through the development, implementation, and maintenance of information protection policies, programs, and plans; coordinates with information resource users to assess information security requirements and to develop and implement information protection procedures; and performs related duties; and performs related work as required.

DISTINGUISHING CHARACTERISTICS OF THE CLASS:
This is journey or full performance level information protection analysis work. It is distinguished from the Information Security Analyst I in that Information Security Analyst II positions are responsible for independently performing duties related to the evaluating, developing, implementing, and monitoring information protection systems with only minimal supervision; whereas Information Security Analyst I positions would be involved in such work only as an assistant to a higher-level analyst. It is distinguished from the Information Security Manager class in that Information Security Manager has full management/supervisory responsibility, whereas Information Security Analyst II does not.

ILLUSTRATIVE DUTIES:
Monitors, analyzes, and evaluates operations and activities to ensure an appropriate level of information protection is achieved and maintained;
Provides maintenance, problem resolution, and analysis of security exposures and opportunities on multiple platforms, including IBM mainframe, UNIX, intranet, internet, NT, network firewalls, and security servers;
Coordinates technical support tasks for the implementation, operation, and maintenance of security applications for software and network systems;
Evaluates security related functions and implements strategies for existing and planned system and network software;
Recommends changes and enhancements as needed to fulfill security requirements;
Coordinates with other staff on the design, implementation, operation, and maintenance of system and network security controls;
Designs and assists in the development, testing, implementation, and maintenance customized modules and for interfaces with other system software;
Assists in the design, development, testing, implementation, and maintenance of system software performing security functions;
Generates security management reports;

Prepares and maintains technical documentation of the system software security functions and implementation strategies and prepares standards and procedures for the administration and operation of security system software;
Monitors software modifications and security controls throughout the system;

Assists in the investigation of attempted or actual security violations;
Trains and advises County and contractor staff in the implementation and use of security system software;
Conducts information protection awareness training sessions;
Trains and advises County and contractor staff in the implementation and use of information protection capabilities;
Prepares, enters, and updates data access permissions in systems;
Provides assistance to other staff as needed;
Provides guidance, training, and technical assistance to less experienced security analysts;
Evaluates technical security products and recommends their acquisition and implementation.

REQUIRED KNOWLEDGE, SKILLS AND ABILITIES:
Knowledge of data security and access control systems, encryption, and related matters;
Knowledge of communications protocols and standards related to security;
Knowledge of information protection methodologies and concepts, such as identification and authentication, access control, inception, and audit trails;
Knowledge of server administration as applied to network and internet security;
Knowledge of information protection standards, guidelines, and applied procedures (i.e., industry "best practices");
Ability to identify potential security breaches and implement counter measures;
Ability to interface with individuals at all levels of the organization and to establish effective working relationships;
Ability to work with sensitive information and maintain confidentiality of such data and information;
Ability to communicate effectively, both orally and in writing;
Ability to provide training and technical assistance to less experienced staff.

EMPLOYMENT STANDARDS:
Any combination of education, experience and training equivalent to the following:
Possession of a bachelor's degree in a computer science field of study, electrical engineering, or telecommunications management; a business degree with computer science coursework; or a bachelor's degree in an associated field of study with coursework in computer science; PLUS
Three years' information systems security experience.

CERTIFICATES AND LICENSES REQUIRED:
None.

ESTABLISHED: May 24, 1999